提供一站式中國網絡安全法–
網絡安全等級保護2.0合規諮詢服務

中國是一個極其重要的市場,對正在中國內地擴張或已在運營的企業而言，其數碼化轉型必須符合最新的法規《中國網路安全法》網絡安全等級保護　2.0。為確保企業可更簡單和順暢地去達到此目的，並得到更嚴格和仔細的驗證，中信國際電訊CPC提供中國網絡安全法 - 網絡安全等級保護 2.0的合規評估服務。此服務一站式涵蓋中國網絡安全法 - 網絡安全等級保護 2.0的所有方面和階段，包括分類、註冊、差異分析、修正和檢測。這項重要服務不僅方便、可靠，更提供專業管理，可保證企業備有強大及完全合規的 網絡安全等級保護 2.0 基礎架構。

合規諮詢服務範圍:

資訊系統調查

中信國際電訊CPC會先進行一個初步的調查,以評估目標的資訊系統,包括公司位置、網絡布局、個人信息類型、現有的信息安全設備和其他設置。

事故後果分類

一旦資訊系統遭到破壞時,跟據網絡安全等級保護2.0級別分類規則會定義事故後果的級別。

註冊所需的資料

所有需要的資料,如合適的文件和表格,都會被妥善準備並提交給當地的警員。

差異分析報告

根據客戶當前的資訊系統布局，而發現的不合規事宜(基於網絡安全等級保護2.0 合規性表格)，我們會為客戶生成"差異分析報告”　。

修正計劃

根據"差異分析報告", 我們會為客戶仔細制定"修正計劃", 幫助客戶以最佳的資訊科技安全手法正確和有系統地填補已識別的安全漏洞。

正式評估援助

我們的專家會協助客戶完成正式評估過程的每一步，以保證客戶的「正式評估報告」最終版本可得到當地網絡警員的批准。

中信國際電訊CPC
CITIC TELECOM CPC

TrustCSI™ 2.0

專業服務

世界一流的安全人才為你服務

› 服務在地 連接全球的數智通訊服務伙伴

中信國際電訊CPC
W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606
荷蘭 T: 31 20 567 2000

TDR2301TC

中信國際電訊(信息技術)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED
中信國際電訊集團成員
A member of CITIC Telecom International

資訊保安專責團隊管理你的重要網絡安全工作

首屈一指的資訊安全人才為您用心服務

無論何等規模的企業現在都在運用數碼轉型的策略以提高生產力和競爭力，且利用尖端技術以增強及擴大其商機。 但是，隨著企業的網絡變得越趨複雜,及市場覆蓋率上升,企業的網絡漏洞也在相應增加。 網路攻擊再不只是流於滋擾,而是會對企業的業務營運,甚至聲譽造成極大損害。 此外,隨著生意的地域擴張,企業需要遵守各種數據和隱私安全的法規,例如《中國網絡安全法》中的要求。

為了協助企業處理和解決以上問題，中信國際電訊CPC的 TrustCSI™專業服務,旨在提供一系列由優秀的信息安全專家去執行的關鍵網絡安全服務,包括漏洞評估、滲透測試、信息安全設備遷移和中國網絡安全法 MLPS 2.0的合規評估。 我們明白聘請世界一流的信息安全專家擔任內部資訊科技人員可能成本高昂,而且並不容易, 但透過TrustCSI™專業服務,任何公司都可以利用中信國際電訊 CPC 內經專業培訓和取得行業認證的信息安全專家的專業知識,以針對解決企業的網絡漏洞, 並協助加強網絡的安全性和支援企業的業務順利地向新地區開展。

TrustCSI™ IAS

深入的TrustCSI™信息評估服務

詳盡分析及透過深入漏洞評估辨識網絡弱點

為徹底分析和識別企業的網絡漏洞,我們的信息安全專家採用四面俱全，以及具系統及規範性的方法,以揭露安全漏洞， 並提供針對企業的網絡安全與對策有效性的洞見。

1

系統性的服務規劃

為確保 TrustCSI™ 信息評估服務可貼合客戶需要，並滿足特定業務和網絡布局的要求，中信國際電訊CPC的認證信息安全專家會先與客戶商討服務的時期及評估範疇。

2

全面的風險評估

為確保所有的信息安全漏洞和風險水平可被準確偵測及評估，TrustCSI™ 信息評估服務利用業界最全面的漏洞知識庫和領先的漏洞管理工具來全面評估網上應用、網絡設備及資訊科技基建。

3

風險報告和建議

對企業的網絡進行了深入分析後，中信國際電訊CPC的信息安全專家會以詳細的報告為企業陳述結果，報告包括所有已被識別的風險(以及一旦透過漏洞入侵的可能後果)。 專家亦會提供建議以堵塞相關漏洞，及提供其他風險修正建議。

4

重新評估

客戶可選擇重新評估服務以作為事後評估。客戶可在此階段檢查更新後的網絡是否已有效堵塞先前的漏洞，及偵測系統有否因資訊科技基建的調整而產生新漏洞。

滲透測試服務助評估資訊安全措施在真實網絡攻擊下的成效

漏洞評估是一個較為被動和分析性的服務項目,相比之下，滲透測試更為主動，即嘗試以駭客角度突破網絡防禦，且集中於攻擊網絡、網上應用和其他企業的應用及接入點上。滲透測試僅是一項無害的模擬測試，目的只為試驗網絡安全措施是否足夠應對模擬現實世界的攻擊。

外部滲透測試

為瞭解網絡攻擊者通過外部攻擊可從獲取哪些企業資訊(公眾或內部),外部滲透測試會在沒有任何內部進入許可的"協助"下進行,以模擬針對網絡數碼資產(例如網上應用、網絡伺服器、網絡端點、VPN、電子郵件伺服器)的攻擊。大多數駭客的攻擊手段皆會在外部滲透測試中被模擬採用。

內部滲透測試

為模擬「內部攻擊」(例如訪客進入企業的範圍內，包括無線範圍、惡意員工或其他內部人員,甚至攻擊者破解外部網絡防禦後獲得的訪問範圍)，內部滲透測試會在企業範圍內進行，集中在電腦設備、內部應用、存取控制、網域名稱和內部文檔上,以識別敏感資訊和控制上的漏洞。

中信國際電訊CPC的信息安全專家會以外部和內部滲透測試練習的結果作為修正建議的基礎。建議內容會向企業客戶現場演示已識別的資產、威脅、漏洞、影響和建議等。

專屬設計信息安全設備遷移服務配合企業資訊安全所需

企業網絡通常隨著業務需求的增長而擴展，企業可能會採用新技術、新營運地點和新的連接方法，包括無線接入。然而， 這些擴展會導致越來越多的切入點和潛在漏洞。中信國際電訊CPC的專業服務團隊可幫助企業遷移信息安全設備至一個度身設計及定做，並更具創新性的信息安全基建，以貼合企業的營運和網絡安全需求。透過詳細的規劃及謹慎的變革管理，信息安全團隊會確保清晰了解原有網絡的風險因素，並解釋優化的遷移策略，以確保流程順暢和可靠。

信息安全設備遷移4步曲

階段1

檢查配置

根據客戶的業務和技術要求，中信國際電訊CPC的信息安全專家會檢查並作出必要的調整,以優化信息安全設備的配置。

階段2

詳細遷移計劃

制定並解釋周詳的遷移步驟、驗證策略和後備計劃。

階段3

實施遷移

順暢的遷移過程可大大減低業務中斷的情況響。經過與客戶的IT團隊協商,中信國際電訊CPC的信息安全專家會幫助規劃遷移的實施時間和整個轉移的時程表。

階段4

最終驗證

當遷移完成後， 中信國際電訊CPC的信息安全專家將驗證一切設備是否運行正常和順暢。